Examiner Search

```
SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC  1969-2002/Dec W2
         (c) 2002 Institution of Electrical Engineers
*File   2: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   6:NTIS  1964-2002/Dec W2
         (c) 2002 NTIS, Intl Cpyrght All Rights Res
*File   6: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   8:Ei Compendex(R)  1970-2002/Nov W4
         (c) 2002 Elsevier Eng.  Info. Inc.
*File   8: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File  34:SciSearch(R) Cited Ref Sci  1990-2002/Dec W2
         (c) 2002 Inst for Sci Info
*File  34: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File  35:Dissertation Abs Online  1861-2002/Nov
         (c) 2002 ProQuest Info&Learning
  File  65:Inside Conferences  1993-2002/Dec W1
         (c) 2002 BLDSC all rts. reserv.
  File  92:IHS Intl.Stds.& Specs.  1999/Nov
         (c) 1999 Information Handling Services
*File 92: This file is closed (no updates)
  File  94:JICST-EPlus  1985-2002/Sep W5
         (c)2002 Japan Science and Tech Corp(JST)
  File  95:TEME-Technology & Management  1989-2002/Nov W4
         (c) 2002 FIZ TECHNIK
  File  99:Wilson Appl. Sci & Tech Abs  1983-2002/Oct
         (c) 2002 The HW Wilson Co.
  File 103:Energy SciTec  1974-2002/Nov B2
         (c) 2002 Contains copyrighted material
*File 103: For access restrictions see Help Restrict.
  File 144:Pascal  1973-2002/Dec W1
         (c) 2002 INIST/CNRS
  File 202:Information Science Abs.  1966-2002/Oct 29
         (c) Information Today, Inc
  File 233:Internet & Personal Comp. Abs.  1981-2002/Nov
         (c) 2002 Info. Today Inc.
  File 239:Mathsci  1940-2002/Jan
         (c) 2002 American Mathematical Society
  File 275:Gale Group Computer DB(TM)  1983-2002/Dec 09
         (c) 2002 The Gale Group
  File 434:SciSearch(R) Cited Ref Sci  1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File 647:CMP  Computer Fulltext  1988-2002/Nov W2
         (c) 2002 CMP Media, LLC
  File 674:Computer News Fulltext  1989-2002/Nov W4
         (c) 2002 IDG Communications
  File 696:DIALOG Telecom. Newsletters  1995-2002/Dec 06
         (c) 2002 The Dialog Corp.

      Set  Items  Description
      ---  -----  -----------
? s (Network or subsystem or or system)(2n)(security or managed or
secure(2n)operations or security(2n)analyst)
>>>Operator "OR" in invalid position
? s (Network or subsystem or system)(2n)(security or managed or
secure(2n)operations or security(2n)analyst)
```

Processing
Processed 10 of [redacted] files ...
Completed processing all files
1920454 NETWORK
81925 SUBSYSTEM
10563736 SYSTEM
364455 SECURITY
146326 MANAGED
118158 SECURE
1071534 OPERATIONS
272 SECURE(2N)OPERATIONS
364455 SECURITY
155753 ANALYST
870 SECURITY(2N)ANALYST
S1 58896 (NETWORK OR SUBSYSTEM OR SYSTEM)(2N)(SECURITY OR MANAGED OR SECURE(2N)OPERATIONS OR SECURITY(2N)ANALYST)
? s s1 and outsource
58896 S1
11306 OUTSOURCE
S2 679 S1 AND OUTSOURCE
? s s2 and intrusion(2n)detect?
679 S2
47269 INTRUSION
3151015 DETECT?
8325 INTRUSION(2N)DETECT?
S3 123 S2 AND INTRUSION(2N)DETECT?
? type s3/full/1

3/9/1 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00668593 02CW08-125
Choosing the best security guards -- IT tackles management issues via service providers
Radcliff, Deborah
Computerworld , August 12, 2002 , v36 n33 p36, 1 Page(s)
ISSN: 0010-4841
Company Name: Counterpane; Internet Security Services; Symantec; Ubizen; Vigilinx
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Talks about managed security services providers (MSSPs). Reports that they address a very real need as information technology departments are drowning in reams of alerts and false alarms coming from various security systems and logs. Explains that at the same time, it is impossible for most companies to hire and keep an expert staff to sort through all of those reports on a daily basis. Shows a table comparing MSSPs Counterpane, Internet Security Services, Riptech, Symantec, Ubizen, and Vigilinx on antivirus, firewalls, **intrusion detection** system, virtual private networks, vulnerability scanning, Web blocking/filtering, monitoring services, incident response and forensics capabilities, and cyberinsurance. Cites savings generated by companies that **outsource** to MSSPs. Includes a table. (MEM)
Descriptors: **Security**; Service Bureaus; **Network Security**; Outsourcing; **Security** Measures; Management
Identifiers: Counterpane; Internet Security Services; Symantec; Ubizen; Vigilinx
? type s3/full/2

3/9/2 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00664138 02NR06-112
Cultivating managed security -- Outsourced security can ease admin. headaches, but issues remain
Messmer, Ellen
Network World , June 10, 2002 , v19 n23 p19-22, 2 Page(s)
ISSN: 0887-7661
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Reports that an increasing number of businesses are choosing to **outsource** the 24-by-7 monitoring of their **intrusion-detection** systems (IDS), firewalls, and virtual private networks (VPNs) to managed security service providers (MSSPs) that do the job remotely over the Internet or private lines. Says that the reason to **outsource** is the difficulty in finding trained personnel to hire for late-night shifts of managing IDS and other security gear, or that in-house costs appear far more than what MSSPs charge to perform the job. Mentions that outsourcing security does not mean abdicating responsibility for security administration. Explains that it requires the customer's information technology (IT) and legal departments to draw up a contract with the MSSP to designate terms and liabilities. Includes a sidebar. (MEM)
Descriptors: **Network Security**; **Security** Measures; Application Service Providers; Service Bureaus; Management; Administration; Outsourcing
? type s3/full/3

3/9/3 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00621530 01NR02-106
Users warming to outsourced **intrusion detection**
Messmer, Ellen
Network World , February 12, 2001 , v18 n7 p36, 1 Page(s)
ISSN: 0887-7661
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses increasing corporate acceptance of the option to **outsource intrusion detection** to Internet service providers (ISPs) and application service providers (ASPs). Reports that while outsourcing security means divulging sensitive information about the corporate network and corporate business practices, some companies say they have little choice but to get outside help given the difficulty of hiring security experts. Says that managing **intrusion-detection** software for customers is a growth area for myCIO.com, the ASP division of Network Associates, Inc. Mentions the Yankee Group's projection that managed security services more than doubled from $200 million in 1999 to $450 million in 2000. Explains that the market will reach $2.6 billion in 2005, fueled by the trend toward outsourcing internal local area **network** (LAN) **security** to professional security firms. Includes a photo. (MEM)
Descriptors: **Security** Measures; Outsourcing; **Network Security**; Enterprise Computing; Application Service Providers; Internet Service Providers
? type s3/full/4

3/9/4 (Item 4 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00621221 01CW02-101
Trust but verify -- Companies can **outsource** their firewalls and **intrusion detection** to save money, but only if they keep an eye on it

Schwartz, Mathew
Computerworld , February 12, 2001 , v35 n7 p58-[illegible] 2 Page(s)
ISSN: 0010-4841
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses outsourced firewalls and **intrusion detection** systems. Mentions that firewalls are part of a greater **network** and **security** infrastructure, which itself derives from a meticulous well-documented security plan. Points out that there are immediate benefits to firewall outsourcing: there are no steep purchase costs, the client does not have to install or maintain the firewall, and it frees network technicians to keep the network running. Explains that outsourced firewalls can be the foundation for security insurance or **intrusion detection** monitoring. Presents steps that the High-Tech Crime Network international president has recommended: realize that managing security is about managing risk; write a thorough security policy; find vendors that ask to see the company's security policy before they make any recommendations; and do penetration testing only if the outsourcer claims to have secured the network. Includes a photo and a sidebar. (MEM)
Descriptors: Firewalls; **Security** Measures; Outsourcing; **Network Security**; Enterprise Computing; **Network** Management
? type s3/full/5

3/9/5 (Item 5 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00618319 01NR01-202
Military mulls battening down net hatches
Messmer, Ellen
Network World , January 15, 2001 , v18 n3 p1, 68, 2 Page(s)
ISSN: 0887-7661
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Reports that the United States Defense Department is developing a policy that would mandate use of round-the-clock **intrusion-detection** systems in all military networks to defend against hacker or denial-of-service attacks. Says that the department could give the military the option to **outsource intrusion detection**. Mentions that by outsourcing **intrusion detection**, the department will go a long way toward legitimizing for the commercial environment the controversial idea of handing over large, sensitive security tasks to service providers. Explains that the military has more than 25,000 computer networks that handle everything from weapons systems command-and-control to inventory to payroll. Offers the suggestion that the option to **outsource** or buy commercial software should be decided on a case-to-case basis. Includes a diagram. (MEM)
Descriptors: **Network Security**; **Security** Measures; Military; Federal Government; Outsourcing; Denial of Service Attacks
? type s3/full/6

3/9/6 (Item 6 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00546556 99IK09-205
Lack security staff? **Outsource** IT
Yasin, Rutrell
InternetWeek , September 20, 1999 , n781 p8, 1 Page(s)
ISSN: 0746-8121
Languages: English
Document Type: Articles, News & Columns

Geographic Location: United States
Reports on the emergence of security services outsourcing in response to the shortage of skilled information technology (IT) professionals. Says that **Network Security** Technologies offers 24-hour monitoring of Internet service provider networks. Notes that Frontier Communications provides antivirus, **intrusion detection**, virtual private network, and firewall functionality. States that Internet Security Systems provides 24-hour network monitoring and management. Says that Comdisco provides security analysis, planning and management. Presents the possibility that demand for such services will increase as companies deploy electronic commerce strategies. Reports on an alliance between Network Associates Inc. and Frontier Communications. Includes one table. (MEM)
Descriptors: Outsourcing; **Security**; Trends; **Network** Management; Personnel
? type s3/full/7

3/9/7 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02656438 SUPPLIER NUMBER: 92788037 (THIS IS THE FULL TEXT)
Security Tutors -- Solution providers are stepping in with services to help customers craft practices and policies that reinforce their technology safeguards.(CRN Security Roundtable discussion)
Savage, Marcia
Computer Reseller News, 16
Oct 14, 2002
ISSN: 0893-8377 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1835 LINE COUNT: 00157

TEXT:
Byline: Marcia Savage

In the world of IT security, there's a plethora of technologies to choose from-firewalls, antivirus protection, **intrusion detection** and encryption, to name a few. Yet the key to securing data and networks lies not in technology but in the human factor, said solution provider executives at the first CRN Security Roundtable in New York.

Although determined hackers and careless users can compromise technology safeguards, security experts can step in with specialized skills and services to help businesses assess and manage their risks and vulnerabilities, as well as develop secure policies and applications, according to roundtable participants, who represented seven firms that sell security solutions and/or services.

"Getting the human in the loop is what it all comes down to," said Chris Ellerman, vice president of professional services at Meridian IT Solutions, Schaumburg, Ill.

The people quotient is becoming ever more critical as the number of security vulnerabilities continues to increase exponentially, roundtable panelists said. And businesses are finding it tough to keep up and are tapping security solution providers to assess their systems on a regular basis, they said.

Dan McCall, executive vice president and co-founder of Guardent, Waltham, Mass., said vulnerability assessments are one of his company's fastest-growing businesses. "We've turned that into a managed service, technology-aided, as an expert looking at the results of automated tools," he said.

While businesses might be able to run scanning tools on their systems to find vulnerabilities, they may not know how to prioritize which security holes are the most critical to fix, the panelists said. "That's the biggest value people get out of our deliverables-the prioritization," said Chris Wysopal, director of research and development at @Stake, Cambridge, Mass.

Any assessment that @Stake does is tied to the business context, comparing the cost of fixing the security problem with the company's business processes, Wysopal said. Companies are now asking for network assessments and penetration tests more often, he added.

"People are saying, 'I need to have these done on a quarterly basis,' where before they might have had it just once a year," Wysopal said.

Paul Rohmeyer, COO of Icons, North Brunswick, N.J., said the growing demand for vulnerability assessments is enabling his firm to turn the assessments into a managed service. "We are implementing scanning architectures and then coming in on a recurring basis to run those architectures and produce findings, coach, train, transfer knowledge-whatever your favorite buzzword is-to leave the client equipped to use those architectures in between our assessments," he said.

Periodic assessments also provide continuous product opportunities, Rohmeyer said. "You're inevitably going to have a better viewpoint of the product needs," he said.

Michelle Drolet, CEO of Conqwest, Holliston, Mass., said her firm provides customers with monthly "health checks"-assessments that employ a variety of tools to check for vulnerabilities and security-policy compliance. About a dozen clients have signed up so far, she said. "We deliver the reports to the IT director, and typically we're brought back in to do a week's worth of remediation," she said.

Conqwest also helps companies train their employees in security policies, such as basic password management. "The weakest link in security, in my mind, is the human factor," Drolet said, explaining that human error is to blame for many security problems.

Other roundtable participants echoed that view. Gary Fish, president and CEO of FishNet Security, Kansas City, Mo., said his firm's services business continues to grow. This year, services account for about 30 percent of FishNet's sales, up from between 15 percent and 20 percent last year, he said. Product sales make up the rest.

"We came up with this new model. We call it APIME: assess, plan, implement, manage and educate," Fish said. "We're going into organizations and saying, 'I could sell you the six firewalls you just asked for, but I'm not sure you really need them. Why don't you let us spend one day (at your company). It will cost $2,500.' We'll do a preliminary assessment, we may run a scan or do a more in-depth assessment, and then we'll write a security road map for that organization."

Recurring assessments are a good fit for companies that don't want to outsource their security entirely to a monitoring firm, said Meridian's Ellerman. For example, Meridian sent an engineer to a client site once a week for six months to help the customer interpret firewall data and implement a security solution, he said.

"They don't want anything going off-site," Ellerman said. "They're looking for a hybrid solution."

The roundtable panelists also said that companies bring them in to assess the security status of organizations that they do business with or plan to acquire. "In B2B contracts, we're being brought in to do security assessments before those people sign the contract to see if they're secure," Conqwest's Drolet said.

And the proliferation of wireless technology is driving additional security assessment work, according to the panelists. Administrators often are embarrassed to discover that someone can drive around in a car rigged with rudimentary equipment and access their corporate data via an unsecured wireless LAN that they didn't even know was in their organization, executives said.

"We're starting to see a lot of requests. They're coming to us and saying, 'We need a wireless audit done,' " Fish said.

Wireless LANs are insecure out of the box, but businesses can implement policies and technology to secure them, solution providers said. "Good security practice is good security practice, across any kind of environment," said Kenneth Cavanagh, vice president of professional services at Vigilinx, Parsippany, N.J. "If (companies) follow the rules and regulations, policies and procedures, wireless can be made as secure as it possibly can be."

@Stake has seen substantial growth in the application assessment and development side of its business, which serves enterprise application developers, ISVs and others, Wysopal said. "People test for functionality and for performance. They don't test for security," he said. "(Security)

should be built into any kind of project."

Finding employees who have the expertise to advise clients on security policies and technology is getting easier, roundtable participants said.

"That churn in the telco business has put an awful lot of talented people back out on the street," Cavanagh said.

This year was the first year that FishNet Security has been able to hire people away from competitors, said Fish, adding that he hired six engineers from competitors that either went out of business or were struggling.

Still, finding people with specific security skills can be a chore, McCall said. "The area where we actually struggle is hiring people that really understand operational security-**intrusion-detection** systems, scanning systems. People who really get it when it comes to firewalls tend to be in very high demand," he said.

Vendor certifications are helpful in managed security because engineers must be able to thoroughly understand specific devices, McCall added.

General security certifications, such as the Certified Information Systems Security Practitioner (CISSP), can demonstrate some technical knowledge and test-taking ability but don't necessarily have hands-on experience, said Cavanagh. He and other panelists said that hiring people with well-honed IT skills is key.

"If you find a good network engineer, and that person can look at a network diagram regardless of what they've been trained in and understand what the security risks and exposures are, then when it comes down to whatever technology is being used in that client environment, they can learn that," Cavanagh said.

Solid IT fundamentals carry much weight in hiring, Wysopal said. "You need to have the basics. Anyone who understands the basics and has an engineering or programming background, it's easy for them to learn the details. It's hard to go the other way," he said.

Customers also are seeking solution providers that not only understand their firewall architectures but also their particular markets, Rohmeyer added. He and other roundtable participants said corporate demand for security expertise is opening up plenty of opportunities for them to provide training services.

"We've been inundated with requests by clients to add training to every project we do," Rohmeyer said. "There seems to be no shortage of training work around."

Added Wysopal: "Everyone wants knowledge transfer, whether it's informal, a few presentations or a primer."

The training @Stake provides is general, covering areas such as secure application design training, according to Wysopal. "We don't teach it for any particular platform," he said.

Some solution providers offer training on specific vendor products. Meridian IT Solutions is a Symantec training center, and FishNet Security is a training center for several vendors, including Check Point Software Technologies and Internet Security Systems.

In some cases, vendors ask solution providers to write training materials, as was the case with FishNet Security and Entercept Security Technologies, Fish said. Likewise, Icons developed an application-security training program for a large vendor, Rohmeyer said.

Looking ahead, roundtable executives said they see no end to the services opportunities in security because it's a never-ending concern.

"The problem is rooted in the dark side of human nature and the complexity of networking. If either of those change in our lifetime, I would be surprised," said Guardent's McCall. "Ultimately, there are going to be technology improvements, but the vulnerabilities will change. What it really requires is some level of service associated with staying on top of it and being diligent about the protection mechanisms."

Bringing together the various departments of a company-human resources, MIS, legal, etc.-to develop and enforce policies is essential to tackling the security problem, Drolet said. "You evaluate, you write the policies, you educate the employees and you put the enforcement technology

in place, and then you start again every month of every quarter," she said. "It's just doing [redacted] diligence."

CRN Security Roundtable
KENNETH CAVANAGH
VP of professional services
Vigilinx
Parsippany, N.J.
Security assessments, intelligence, managed security services
MICHELLE DROLET
CEO
Conqwest
Holliston, Mass.
Security assessments, policy development, infrastructure design
CHRIS ELLERMAN
VP of professional services
Meridian IT Solutions
Schaumburg, Ill.
Network infrastructure solutions, with a security specialty
GARY FISH
President and CEO
FishNet Security
Kansas City, Mo.
Security integration and support, with government and health-care practices
DAN MCCALL
Executive VP & co-founder
Guardent
Waltham, Mass.
Managed security services, security consulting
PAUL ROHMEYER
COO
Icons
North Brunswick, N.J.
Security consulting, vulnerability assessments, application security, **intrusion-detection** systems
CHRIS WYSOPAL
Director of R&D
@stake
Cambridge, Mass.
Security consulting, **network** and application assessments, incident response, forensics
http://www.crn.com

DESCRIPTORS: Information technology
EVENT CODES/NAMES: 260 General services
PRODUCT/INDUSTRY NAMES: 9912600 (Information Systems & Theory)
FILE SEGMENT: CD File 275
? type s3/full/8

3/9/8 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02641069 SUPPLIER NUMBER: 91263786 (THIS IS THE FULL TEXT)
Focus on Identity, Vigilance.
eWeek, NA
Sept 9, 2002
ISSN: 1530-6283 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1209 LINE COUNT: 00105

TEXT:

The terrori[redacted]attacks of last september perm[redacted]ntly changed the terms of debate for subsequent discussions of IT security and the technical response to potential terrorist threats.

Almost no imaginable attack can now be dismissed, and it is no longer a confession of incompetence to acknowledge that at least some attacks will succeed.

Some technologies were unduly demonized in September's aftermath. For example, there was an immediate flurry of ill-conceived proposals to attempt restrictions on access to encryption. Thankfully, this notion is no longer holding sway among even the most ill-informed legislators or the most opportunistic enforcement agencies.

As noted in February's position statement from the IEEE, "Encryption is likely to be used by criminals to protect their communications, but their use of encryption is not necessarily obvious. ... Laws prohibiting the use of unescrowed, strong encryption would be of little use to law enforcement efforts."

Any broad use of Web services will depend on well-integrated encryption; distributed storage and processing solutions must also incorporate encryption to protect data and real-time business intelligence.

Enterprises should, therefore, be developing internal guidelines--and monitoring relevant industry standards and regulatory requirements--to strike a balance between the desired degree and duration of cryptographic protection and the performance overhead and costs of processor-intensive crypto algorithms.

Other technologies enjoyed brief moments in the spotlight of our hopes for a quick technology fix. Face recognition, for example, can be quite effective under controlled conditions, but tests in public airport security checkpoints during the past year have been disappointing. Tests in Palm Beach, Fla., this spring and in Boston this summer failed to limit false alarms to acceptable levels while still consistently recognizing "suspects" (played by airport employees).

More intrusive technologies, such as eye and fingerprint matching, have also failed to live up to their hype. Strategies as simple as breathing on a fingerprint scanner, making the previous user's fingerprint reappear to be re-scanned, are dismayingly effective.

Prices for iris scanners, which are harder to fool and less likely to falsely reject legitimate users, are coming down into the same $100-plus price range as fingerprint scanners, but administrative issues still impede adoption: In eWeek Labs' review of the Panasonic Biometric Group's Authenticam, for example, we found the included software far better suited to individual workstation access control than to large-scale **network security**. (For more on the use of biometrics, see story, left.)

Rather than pushing the envelope of cost, not to mention possible user discomfort with the "Minority Report" aura of pervasive biometrics, enterprises will do better to streamline their identity management systems. This means integrating e-mail, voice mail, workflow and file-sharing systems under well-defined privilege management schemes, rather than devoting resources to elaborate and conspicuous "gee-whiz" hardware.

USA Patriot Act

Hopes remain high, though, for following terrorists' footprints--not the kind left by shoes but the kind left in cyberspace by travel arrangements and other financial transactions.

The USA Patriot Act, signed into law last October, is named with a tortured acronym: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (doubly condensed to USAPA).

The USAPA itself consists largely of revisions to other laws. The burden falls on ISPs, financial institutions and other potential targets of expanded subpoena powers to understand the aggregate effect on their resulting obligations.

Individuals and enterprises should also understand the effect of USAPA on the exposure of their records, electronic communications (including voice mail) and other information assets--especially to the extent that these are handled or stored by third parties.

Enterprises and **outsource** providers should conduct a complete review of their respective rights and obligations, especially to the degree that their service contracts and confidentiality agreements may be vitiated by subpoenas or court orders.

Focus on Identity

Enterprise IT architects in the year since Sept. 11 have also been hard pressed to cope with a flood of urgent items in more familiar domains, such as network operating systems, firewalls, virtual private networks, **intrusion detection** systems and anti-virus tools. The following trends are apparent.

Perimeter defense, as a viable strategy, is dead. Wireless and nomadic laptop devices, with external network connections, make it impossible to define even the physical location of the network edge. Web services make the logical location still harder to characterize.

Network protection must, therefore, focus on identities and privileges of authorized users, using tools such as Zone Labs Inc.'s Integrity. During our review this spring, we found the product (priced at $80 per user with volume discounts) effective in controlling client devices' Internet access on an application-specific basis.

The pervasive network can be its own worst enemy in the ease with which it propagates virus attacks. Enlisting the network in its own defense are products such as Network Associates Inc.'s McAfee Security VirusScan ASaP, which uses peer-to-peer technology.

Meanwhile, key IT vendors have been addressing concerns about out-of-the-box insecurity with a long-overdue shift toward more secure default configurations. In our tests last month of Microsoft Corp.'s Windows .Net Server Release Candidate 1, for example, we found that the installer utility detected our failure to run the Internet Information Services Lockdown Wizard and automatically disabled IIS.

Our pleasure was limited, though, by the discovery that restarting the server did not trigger any further notice of our exposures--notably, the many default extensions retained from our previous Windows 2000 installation. On the plus side, installation of .Net Server on a bare machine gave us ample warning of bad practices, such as leaving an Administrator password blank.

Poor administrative practices wouldn't be such an open invitation to attackers if systems didn't grant unrestricted superuser status. We remain strong advocates of the trusted-system architecture in products such as Argus Systems Group Inc.'s PitBull, the only technology that has yet survived one of our international Openhack events unscathed--though a successful attack on the underlying operating system kernel, specifically on a version of Solaris 7 x86, did succeed in a challenge late last year.

The message here is that every security technology--regardless of architectural merits--demands continued vigilance. That vigilance is embodied in state-of-the-art **intrusion detection** in products such as OneSecure Inc.'s **Intrusion Detection** and Protection appliance. Rather than merely relying on known attack signatures, the $16,495 OneSecure device (which we reviewed last month) uses various heuristics to detect previously uncharacterized attacks. By developing a model of normal traffic and using sophisticated analysis of attack patterns, the **Intrusion Detection** and Protection appliance can identify new threats while minimizing the time lost to false alarms--the goal, we're sure, of every IT administrator a year after Sept. 11.

Technology Editor Peter Coffee can be reached at peter_coffee@ziffdavis.com. The reviews cited in this story can be accessed at www.eweek.com/links

GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Management issue; MIS
EVENT CODES/NAMES: 220 Strategy & planning
PRODUCT/INDUSTRY NAMES: 3573021 (Management Information Systems (Computers))
SIC CODES: 3571 Electronic computers
NAICS CODES: 334111 Electronic Computer Manufacturing

FILE SEGMENT: CD File 275
? type s3/full/10

3/9/100 (Item 23 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01196112 CMP ACCESSION NUMBER: IWK19990712S0038
Global Security Survey Virus Attack
Amy K. Larsen
INFORMATIONWEEK, 1999, n 743, PG42
PUBLICATION DATE: 990712
JOURNAL CODE: IWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Trends
WORD COUNT: 3457
TEXT:

In the last several months, two nasty E-mail viruses-one called Melissa and another known as Worm-rode the Internet and infected E- mail systems worldwide, clogging networks and hard drives and in some cases destroying data. Scores of companies had to shut down systems and networks in order to rid themselves of the problem.

St. Barnabas Healthcare System was one of those companies hit by Melissa. Virus-scanning software it was testing caught the problem before it became serious, but the experience gave the company a new perspective on viruses. "Viruses used to be like a mosquito bite to most companies. Now they look like malaria," says Tony Macaluso, VP of technology resources and chief technology officer for the Toms River, N.J., health-care company.

Viruses, which represent the single biggest computer and **network security** concern among business, are a growing problem, according toInformationWeek's Global Information Security Survey, conducted with PricewaterhouseCoopers LLP. Released this week, the survey is based on responses from 2,700 executives, security professionals, and technology managers from 49 countries (for the methodology used, see p. 48; for complete results, go to www.informationweek.com/743/ secure.htm). Even with new, more advanced security available, companies are still vulnerable. Global networks, Internet technologies , and a demanding pace of change are putting companies at risk.

Globally, about 64% of companies were hit by at least one virus in the past 12 months, up from 53% the year before. In the United States, viruses stung 69% of companies. Those figures are about four times as high as the next highest category of **security** breaches: unauthorized **network** entry.

Most other forms of security problems declined or remained flat in the past year, with reports of information loss dropping from 15% of respondents to 11%; data and system integrity losses falling from 14% to 11%; and denial of service declining from 13% to 11% (see chart, left).

The only category of security problem other than viruses to show an increase this year is Trojan horses, which mimic familiar programs to trick users' into divulging passwords and other key information. The number of companies reporting Trojan horses jumped from 3% to 8%.

The percentage of companies suffering security breaches increased slightly. Last year, 27% of companies responding said they had not suffered a security breach. This year, only 24% could make that claim. In the United States, just 22% reported no security breaches.

It's hard to know exactly who is responsible for security breaches. But when asked who they suspected was responsible, survey respondents

cited computer hackers or terrorists as the leading cause. A year ago , only 14% named hackers and terrorists as the probable cause of breaches and espionage; this year, that number jumped to 48%. Respondents also pointed to contract service providers, which were named by 31% of respondents this year compared with 9% a year ago.

"Many companies in the past would never have known that they'd been hacked by outsiders," explains Mark Lobel, a manager of technology risk services for PricewaterhouseCoopers. "But the growing use of **intrusion-detection** systems and other security programs means they can now better identify the cause of their problems."

The good news: Fewer respondents blamed authorized users and employees for their security problems, down to 41% this year from 58% last year (see chart, p. 44).

The growth in outsourcing is probably the main reason more IT mangers cited contracted service providers as a suspected threat and fewer named their own employees, Lobel says. "These contractors have the same motivation and means as in-house employees. I know of one outside contractor who, when he heard that he was losing the job, started installing the 90-day trial version of Windows NT as his form of revenge."

Overall, security problems are becoming more serious. A year ago, half of the companies surveyed said they suffered no system downtime as a result of security breaches. This year, only 36% could make that claim (see chart, p. 48).

Viruses attack just about everybody equally. While noncommercial organizations with limited IT budgets are frequent virus victims-78% of educational groups and 74% of government respondents reported being infected-large and better-financed companies didn't enjoy significantly greater immunity: Viruses hit 69% of companies with revenue of more than $500 million. Despite the growing threat from Internet-borne viruses and online virus-building toolkits, the survey shows that about 5% of responding companies still don't have antivirus software in place.

The virus fear factor is causing some companies to look at malicious code in a new light- especially in the wake of the Melissa and Worm viruses that ruined users' hard drives.

At St. Barnabas, the close encounter with Melissa and the growing presence of other damaging viruses has caused the company to reassess how it fights those threats. Until about six months ago, the 130-site health-care company classified antivirus scanning as a utility, separate from other security functions. St. Barnabas now counts a virus attack as a breach and deals with it as a security threat.

"We had a view of the world that put antivirus in a separate silo from **intrusion detection**, and that was separate from another security function," VP Macaluso says. "Now we're trying to consolidate all those functions as part of a centralized access control and authentication system."

St. Barnabas is implementing an integrated **security system** that includes capabilities such as single sign-on and antivirus software, and Macaluso hopes the resulting comprehensive system will be more effective than using individual security systems. To accomplish that, St. Barnabas turned to Computer Associates for help. When the Melissa virus struck, the health-care company was testing CA's InoculateIT, which uses heuristic scanning, a kind of artificial intelligence that identifies unknown viruses. The CA software spotted the virus quickly and the IT staff at St. Barnabas was able to contain it without shutting down its entire network, Macaluso says.

No Assurances

Businesses that have managed to avoid or contain security breaches in the past shouldn't rest easy, IT managers and security experts say. No company is immune. "The longer you go without a security breach, the closer you are to your next incident," says Ken Shaurette, information security staff adviser for American Family Insurance in Madison, Wis.

IT managers need to fully understand the threat before they can effectively determine ways to protect their systems. Being able to identify how a security breach took place and who initiated it is crucial to preventing future unauthorized access and tampering. "You need to tighten all the joints before you can have truly effective security," says PricewaterhouseCoopers' Lobel.

On this point, there's good news. Most companies are doing an effective job of tracing breaches to identify how an attack took place , the survey indicates. Only 13% of respondents were unable to name what kinds of security breaches hit their networks, down from 20% a year ago.

Outsiders are the main cause of security problems, survey respondents say. How do they know that? More companies are using **intrusion-detection** systems that scan the network for trespassers and alert IT personnel in real time if intruders are discovered. This year , 37% of survey respondents reported using **intrusion-detection** products, up from 29% last year. And every company that said it uses **intrusion-detection** systems discovered unwelcome outsiders prowling in their systems.

"That 100% of users were able to catch intrusions with (**intrusion- detection** system) is a testament that they actually work," says PricewaterhouseCoopers' Lobel. The effectiveness and growing ease of use of **intrusion-detection** systems has helped fuel their use. "People are looking for less manually intensive and less reactive tools so they can deal with incidents in real time," Lobel adds.

The tools are designed to help IT managers save time, which is important because lack of time was cited as the main barrier to implementing improved security. The time-crunch problem, however, is not as serious as it was last year (see chart, p. 52).

Of course, security products are useless unless they work in tandem with effective policies. "Technology by itself can't eliminate exposure," American Family Insurance's Shaurette says. "To do that, you need some supporting structures that become the policies."

Survey respondents, however, say that setting security policies to match business goals is difficult and, in many cases, the two aren't in sync. Only 41% say their policies are very much in line with their business objectives. On average, survey respondents rate their alignment of policy and business goals at just 6.5 on a scale of 1 to 10, with 10 being the highest.

That view is reinforced by the fact that only 31% of respondents describe their security policies as highly effective, while 19% say their policies are basically ineffective. Fewer companies are even attempting to measure the effectiveness of their security policies. This year, 27% say their companies are tracking the effectiveness of their security policies, down from 34% last year.

One challenge that security professionals face in establishing policies is striking a balance between being overly cautious on the one hand and lax on the other. "It's easy to straddle that line," says American Family Insurance's Shaurette. "What has to happen is security has to become a function of the corporation, not an obstacle to business."

And without the involvement of high-level management in making, communicating, and enforcing security policies, there's only a limited chance of success, analysts and IT managers say.

The survey shows that 81% of companies with security policies make an effort to communicate those policies to their employees (see chart, p. 50). American Family Insurance, for example, employs 9,000 staff members plus an additional 10,000 exclusive affiliate agents and support personnel in 14 states. The company says it actively engages in security discussions with its employees and agents.

Security is growing as a priority. Information security ranked as a priority in 60% of the companies responding to the survey, up 56% from last year. Despite that ranking, information security still gets shortchanged by many companies, including large enterprises. The survey shows that 33% of companies with more than $500 million in annual revenue are spending less than $100,000 this year on security, including staffing, consulting, and technology. Overall, however, the survey shows that most companies are spending more money on security than they did last year (see chart, p. 56).

As enterprise networks and systems become more extensive and complicated, providing effective security becomes more difficult. Threats can come from many directions and can be aimed at a variety of potential weak points. That has turned security-from both technical and process points of view-into a multilayered equation that covers everything from network devices to applications.

As a result, companies have been forced to use a variety of methods to ensure that only an authorized person can gain access to a network , system, or application. Passwords remain the most widely used technique to validate the identity of a users, with 65% of survey respondents using multiple logons or passwords to limit access to applications.

The survey shows that protecting a network from unauthorized access is by far the top priority for most companies, with more than 90% of respondents saying their companies focus security spending on preventing outsiders from gaining access to their systems. The No. 2 priority is protecting key data.

Some companies layer security systems one on top of another in order to make unauthorized access more difficult, but some IT managers say that approach isn't the most effective way to secure an entire system. "Each layer of protection is a separate card in a house of cards," says American Family Insurance's Shaurette. "Adding an extra card to the house doesn't necessarily make the house stronger."

The most effective way to secure a business application is to build or develop the application and its protective components together, experts say. Too often, security is added to business applications after the fact. However, a growing number of electronic-commerce apps are being built with security as part of the design.

Take the example of Bally's Gaming and Systems online sports gambling service, to be launched later this summer. Bally's, already a major player in the $600 billion-a-year casino business, wants to tap into the emerging online gambling market, which is expected to grow to $2 billion by 2003. But before the company can enter the new market , it has to meet certain security requirements.

Security is an integral part of Bally's wagering application because the law says it has to be. In addition to the normal protective measures an online company must take to conduct business over the Web, the gambling company is legally required to authenticate not just who places

bets online but what jurisdiction they are in when they access the wagering system. [redacted] had our security specificati[redacted] mapped out before we even knew exactly what the application was going to be," says Tony Fontaine, VP of applied technology for Bally's.

The law prevents the company from starting a wagering system on the Internet, so Bally's created a private intranet application that members can access via browsers to place bets on sporting events. Because only people 18 and older can gamble legally, Bally's first needs to authenticate a person's age and that the person attempting to access the system is actually a member of its private **system**.

Security Requirements

Implementing a system that satisfied Bally's own security needs as well as the legal requirements wasn't easy. To become a member, a potential player must first go in person to a casino office, show proof of age, and then open an account with a cash deposit. Gamblers can only wager up to the amount of money held in trust for them by the casino.

Members receive software to load onto their PCs, a smart card with their personal identification information, and a smart-card reader. Before players can enter the online casino, they have to enter their log-ons and passwords, then answer a variety of questions. All of the transmitted information is encrypted using a proprietary cryptographic scheme. Once members make it through that exchange, they are allowed access to the network-but not to the gambling application itself.

Bally's is bound by gambling laws that vary by jurisdiction, so the system has to verify the member's location. The application essentially traces the call and compares the phone number to a table of exchanges in areas where gambling is legal. Fontaine says Bally's is interested in other emerging techniques, such as biometrics that authenticate a user's identity based on unique traits such as a fingerprint.

Biometric technology also appeals to Blueline Online, a building project management portal. The Palo Alto, Calif., company runs an Internet collaboration system that construction companies and their subcontractors can use to share project design and other building information.

"The liability issues in construction are unbelievable," says Ashok Segu, chief technology officer and VP of engineering for Blueline Online. "If it takes two years to build a building, it takes 20 years to get out of it legally. Construction is a very litigious industry."

Using biometric measures such as fingerprints to create and validate an audit trail would be very helpful, Segu says. But the expense and immaturity of biometric technology keep Blueline Online from investing in it now. Instead, the portal company uses database access records, including date and time information, to create an audit trail.

While preventing unauthorized access and verifying the identity of those who do gain access are among the top priorities of many companies, a growing number are recognizing the importance of taking direct steps to protect their data. About 60% of the respondents use some form of cryptography to scramble data so it's useless to anyone but those authorized to see it. "Cryptography is the enabler of E- business," says PricewaterhouseCoopers' Lobel. "People are really starting to get it."

The skyrocketing growth of applications such as electronic commerce and Web hosting presents IT managers with a new challenge: how to maintain security standards while giving customers or business partners access to systems. One approach that's becoming more popular is the use of virtual private networks, which create secure, encrypted transmission tunnels to carry business data over private and public IP networks. Use of VPNs to

transmit data securely rose to 27% this year, up from from 11% in last year's survey.

Blueline Online uses Pilot Network Services' hosted VPN to secure the connections between the construction companies and subcontractors that use its site.

"We were still a small company when we started out in 1997. We looked at managing our own VPN, but it made more sense to **outsource** it ," says Segu. "For our customers, it's almost like putting the crown jewels in a bank. You have to ask how well you know the bank. Since we were new, no one knew us that well. So it seemed logical to go with a service provider that specializes in VPNs."

In the United States, VPNs are particularly popular as an inexpensive way to connect remote users to the enterprise. PricewaterhouseCoopers is in the process of deploying a VPN to link 35,000 remote-access workers to its network. The cost savings comes from eliminating long-distance calls. With a VPN, remote workers make a local call to an Internet service provider to connect to the company network via the Internet, rather than making a long-distance call to the company's modem pool.

Some 30% of respondents say they use Secure Sockets Layer, a communications protocol developed by Netscape to encrypt data during transmission from a client to a server. A common part

of E-commerce transactions, SSL encrypts data in transit between the client and server, but doesn't rescramble the data at the server itself.

More sophisticated cryptographic schemes such as public key infrastructure technology are gaining momentum. The number of companies using PKI software more than doubled from 6% a year ago to 13% this year, according to the survey. PKI software uses a string of numbers or keys to encrypt documents to protect them from unauthorized access and then decrypt them for authenticated users.

The system relies on certificate authorities, organizations that store in a database public keys that can be used to verify that the sender of a message or data is who he or she claims to be, and that the person who receives the message or data is the intended recipient. The certificate authority creates a digital certificate that verifies the sender's identity and that the document wasn't altered in transit.

Not surprisingly, industries that make the greatest use of encryption include banking (28% of data traffic is encrypted), telecommunications (24%), financial (24%), and computer (24%). Industries that encrypt 15% or less of their data traffic include insurance, retail, manufacturing, aerospace, transportation, energy and utilities, and education.

Many respondents-40%-don't bother to classify their most sensitive data files and records. Of the 60% of respondents who say they do classify important data, 18% do it daily, 6% weekly, 10% monthly, 15% annually, and 11% occasionally.

"Classifying data is pretty labor intensive," says Shaurette of American Family Insurance. Even companies that do categorize documents by security requirements only do so with the most sensitive documents , he says, and few bother to classify fields within a document such as Social Security or credit-card numbers.

In most cases, companies concentrate on protecting information in transit, Shaurette says, and that doesn't go far enough. "Data security

implies securing something that is electronic," he says. "But it is information that is really valuable to the business, not pure data-so we need to put security practices in place that protect information when it is printed out and sitting on someone's desk or displayed on their screen."

Of course, monitoring how users treat information is made more difficult by the increased sharing of data between companies that are supply-chain partners or using an industrywide extranet. Shaurette says communications about security policies-to users, partners, and suppliers-is essential.

Commitment From Above

For that kind of communication to become part of a company's culture, it takes a high-level commitment. The CIO, a VP, or a director of IS or IT is the one who sets the security policy at 52% of companies surveyed. And 47% say that same executive determines security spending levels. Interestingly, 30% say their company president, CEO, or managing director sets security policies, and 36% said the top executive sets security spending.

This seems to indicate that growing numbers of upper-level managers realize that to keep a business running smoothly requires creating and supporting a secure information infrastructure. That, in turn, means tying together policy, practices, and people through communication and execution.

"When it comes down to it, the biggest risk is ignorance," Shaurette says. "Actually, it's the only risk. Ignorance is what ties together all the exposures that exist."

COMPANY NAMES (DIALOG GENERATED): American Family Insurance ; Bally ; Blueline Online ; Computer Associates ; IS ; IT ; Pilot Network Services ; PricewaterhouseCoopers ; Social Security

? type s3/full/106

3/9/106 (Item 29 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01171065 CMP ACCESSION NUMBER: VAR19980831S0021
Taking an Integrated Approach To Security - Empower Your Clients To Monitor Their Networks With Adaptive Security Management
Jackie Poole; Associate Editor
VARBUSINESS, 1998, n 1418, PG43
PUBLICATION DATE: 980831
JOURNAL CODE: VAR LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Technology - Internet
WORD COUNT: 897
TEXT:

These days, companies are looking closely at ways to leverage the Internet to gain a competitive advantage-either through e-commerce or information delivery-and it has caused the market for security products to catch on like wildfire. A new breed of security products called adaptive security management software is the most recent to join the party. These products augment the traditional safeguards, such as firewalls, which also serve as a hook for VARs to amass additional sales and service revenue. The Yankee Group, a Boston consulting firm, estimates the market for adaptive security management products at $160 million in 1998, $315 million in 1999 and $679 million by 2002.

The issue at hand is a security challenge, which results from the increased use of open systems and the rapid integration of Internet

technology into networks, says Chris Rossie, vice president of channel operations at Atlanta-based Internet Security Systems Inc. (ISS). Security threats are growing from the inside and the outside, but most companies have limited security resources and expertise, says Rossie. The opportunity for the channel is to integrate security safeguards, such as access control, firewalls, authentication and encryption, along with adaptive security management products, such as those from ISS. Those products can help the traditional safeguards work better. Adaptive security management applies a proactive approach, which consists of monitoring, detection and response.

"We help organizations understand what risks they have according to a risk model: Risk equals Vulnerability times Threat equals Value. Managing business risk is about managing vulnerability and threats to an acceptable level," says Rossie. Vulnerability can take the form of software bugs, misconfigurations and enabled, but unused, services. Threats are people who use those vulnerabilities to break into a network, either from the inside or the outside. Many companies are beginning to realize that threats consist not only of "wily hackers" on the outside of the company, but also those from within. These days, companies need to pay close attention to the network activities of employees, contractors and those with whom they work on an **outsource** basis.

Adaptive security technology from ISS includes proactive and reactive products, such as Internet Scanner, which detects and corrects vulnerability on the network, and System Scanner, which does the same at the system level. RealSecure handles **intrusion detection** and responds to threats on the network. It sits either in front of or behind a firewall.

One analyst says firewalls alone provide companies with a false sense of security. "If you put up a firewall, you identify a way in, and hackers are better equipped to break into your network," says Matthew Kovar, senior analyst at The Yankee Group. "A firewall is only as good as the implementation."

Typically, companies have safeguards at the perimeter of their businesses to protect against external threats. VARs will be able to use those perimeter measures as springboards to implement adaptive security, says Rossie. VARs can draw revenue from product sales, services and from training their customers. "If there is a vulnerability in the firewall, the products can correct it. If a threat is identified at the firewall, the products can reconfigure the firewall. This is the main difference between static and adaptive security," says Rossie.

Jay Johnson, vice president of operations at VAR SecureIT Inc., Norcross, Ga., says the goal is to educate clients so they can be self-sufficient on security. In most cases, this is unrealistic because security changes so fast. "It's hard to stay on top of all the security holes. You can't resolve them all, so you have to put in a 'hall monitor,"' he says. Johnson says his company takes the nonthreatening approach with customers rather than punching a hole in their security and showing them how easily a hacker could do the same. He shows clients that the problem is technology and not their security device, and what they need to take every precaution.

Among the vendors leading the charge are ISS, with 30 percent of the market, followed by Axent Technologies Inc. with 19 percent, and Network Associates Inc. and Cisco Systems Inc. with 11 percent each, according to The Yankee Group's 1997 research. VAR SecureIT has been working with ISS products and implementing them for clients across a range of verticals, including utilities, financial, telecommunications , state and local governments. Some clients take a proactive approach, while others are reacting to a breach of security. Johnson explains that for the latter, it is an unfortunate and painful learning process. Most people

don't budget enough money to security until there is a "significant emotional event," [redacted] until you show them that you can exploit a vulnerability, he says.

Security safeguards have often been implemented on a departmental level, says Rossie. Security is becoming increasingly enterprise- oriented. The decision-making process is changing accordingly: Budget dollars come from one department and the decision comes from another. And yet, the implementation affects a third department. Therefore, security is becoming more complex, and VARs have to position themselves to go after those types of opportunities.

-Quick Scan

Artisoft Inc. Tucson, Ariz. (520) 670-7100, www.artisoft.com

Axent Technologies Inc. Rockville, Md. (301) 330-5756, www.axent.com

Check Point Software Technologies Inc. Redwood City, Calif. (650) 628-2000, www.checkpoint.com

Cisco Systems Inc. San Jose, Calif. (408) 526-4000, www.cisco.com

Internet Security Systems Inc. Atlanta, Ga. (678) 943-6000, www.iss.net

Network Associates Inc. Santa Clara, Calif. (408) 988-3832, www.networkassociates.com